Source Code Analysis Tools - References

Cigital, Inc.

2006-06-12; Updated 2009-02-16 by Howard F. Lipson[1]

Content area bibliography.

See also Code Analysis - References[2]

"A Comparative Study of Industrial Static Analysis Tools." Emanuelsson, Par and Nilsson, Ulf. *Electronic Notes in Theoretical Computer Science*, Vol. 217, No. C, July 21, 2008, pp. 5-21, Elsevier.

"A Comparison of Publicly Available Tools for Static Buffer Overflow Prevention[3]." Wilander, John and Kamkar, Mariam, *Proceedings of the 7th Nordic Workshop on Secure IT Systems*, 2002.

"A Lightweight Security Analyzer Inside GCC." Pozza, D. and Sisto, R. *2008 3rd International Conference on Availability, Reliability and Security (ARES '08)*, pp. 851-8, March 4-7, 2008, Barcelona, Spain, IEEE Computer Society.

"Comparing Lexical Analysis Tools for Buffer Overflow Detection in Network Software." Pozza, Davide, Sisto, Riccardo, Durante, Luca, and Valenzano, Adriano, *First International Conference on Communication System Software and Middleware*, Comsware 2006, Jan. 8-12, 2006, New Delhi, India, IEEE Computer Society.

"Dynamic Buffer Overflow Detection[4]." Zhivich, Michael, Leek, Tim, and Lippmann, Richard, *Workshop on the Evaluation of Software Defect Detection Tools*[5], 2005.

"Effect of Static Analysis Tools on Software Security: Preliminary Investigation[6]." Okun, Vadim, Guthrie, William F., Gaucher, Romain, and Black, Paul E., *Third Workshop on Quality of Protection* (QoP), Oct. 2007.

"Evaluating Static Analysis Defect Warnings on Production Software." Ayewah, Nathaniel, Pugh, William, Morgenthaler, J. David, Penix, John, and Zhou, Yuqian, *PASTE'07 - Proceedings of the 7th ACM SIGPLAN-SIGSOFT Workshop on Program Analysis for Software Tools and Engineering*, pp. 1-7, June 13-14, 2007, San Diego, CA, Association for Computing Machinery, 2007.

"Evaluating Static Analysis Tools for Detecting Buffer Overflows in C Code." Kratkiewicz, Kendra, Master's Thesis, Harvard University, 2005.

"Evaluating the Cost Reduction of Static Code Analysis for Software Security." Baca, Dejan, Carlsson, Bengt, and Lundberg, Lars, *Proceedings of the ACM SIGPLAN 3rd Workshop on Programming Languages and Analysis for Security (PLAS'08)*, pp. 79-88, June 8, 2008, Tucson, AZ, Association for Computing Machinery.

"Improving Software Quality with Static Analysis." Foster, Jeffrey S., Hicks, Michael W., and Pugh, William. *Proceedings of the 7th ACM SIGPLAN/SIGSOFT Workshop on Program Analysis for Software Tools and Engineering* (*PASTE'07)*, pp. 83-84, June 13-14, 2007, San Diego, CA, Association for Computing Machinery.

"Maximising the Information Gained from a Study of Static Analysis Technologies for Concurrent Software." Wojcicki, Margaret A. and Strooper, Paul, *Empirical Software Engineering*, Vol. 12, No. 6 (Dec. 2007), pp. 617-645, Kluwer Academic Publishers.

[1] http://buildsecurityin.us-cert.gov/bsi/about_us/authors/15-BSI.html (Lipson, Howard F.)

[2] http://buildsecurityin.us-cert.gov/bsi/articles/best-practices/code/213-BSI.html (Code Analysis - References)

[3] http://www.ida.liu.se/%7Ejohwi/research_publications/paper_ndss2003_john_wilander.pdf

[4] http://www.cs.umd.edu/%7Epugh/BugWorkshop05/papers/61-zhivich.pdf

[5] http://www.cs.umd.edu/%7Epugh/BugWorkshop05

[6] http://samate.nist.gov/docs/SA_tool_effect_QoP.pdf

NIST Software Assurance Metrics And Tool Evaluation[7] (SAMATE) Project

"On the Use of Data Flow Analysis in Static Profiling." Boogerd, C. and Moonen, L. *2008 Eighth IEEE International Working Conference on Source Code Analysis and Manipulation (SCAM 2008)*, pp. 79-88, Sept. 28-29, 2008, Beijing, China, IEEE Computer Society.

"On the Value of Static Analysis for Fault Detection in Software." Zheng, J., Williams, L., Nagappan, N., Snipes, W., Hudepohl, J. P., and Vouk, M.A., *IEEE Transactions on Software Engineering*, Vol. 32, No. 4, April 2006, pp. 240-53, IEEE Computer Society.

"Predicting Software Defect Density: A Case Study on Automated Static Code Analysis." Marchenko, Artem and Abrahamsson, Pekka, *Lecture Notes in Computer Science*, Vol. 4536 LNCS, *Proceedings, Agile Processes in Software Engineering and Extreme Programming - 8th International Conference (XP 2007),* pp. 137-140, June 18-22, 2007, Como, Italy, Springer Verlag.

Proceedings - 8th IEEE International Working Conference on Source Code Analysis and Manipulation (SCAM 2008), 2008, Sept. 28-29, 2008, Beijing, China, IEEE Computer Society.

Proceedings - 7th IEEE International Working Conference on Source Code Analysis and Manipulation (SCAM 2007), Sept. 30-Oct. 1, 2007, Paris, France, IEEE Computer Society.

Proceedings - 6th IEEE International Workshop on Source Code Analysis and Manipulation (SCAM 2006), Sept. 27-29, 2006, Philadelphia, PA, USA, IEEE Computer Society.

Proceedings of the Static Analysis Workshop, SAW 2008, June 12, 2008, Tucson, AZ, Association for Computing Machinery.

"Putting the Tools to Work: How to Succeed with Source Code Analysis." Chandra, Pravir and Chess, Brian, *IEEE Security and Privacy*, Vol. 4, No. 3 (May/June 2006), pp. 80-83, IEEE Computer Society.

"SAMATE and Evaluating Static Analysis Tools." Black, Paul E., *Ada User Journal*, Vol. 28, No. 3, Sept. 2007, pp. 184-8, Ada Language UK Ltd., UK.

"SAMATE and Evaluating Static Analysis Tools[8]." Black, Paul E., *International Conference on Reliable Software Technologies* - Ada-Europe, June 2007.

"Securing Java Code: Heuristics and an Evaluation of Static Analysis Tools." Ware, Michael S. and Fox, Christopher J., *Proceedings of the Static Analysis Workshop* (SAW 2008), pp. 12-21, June 12, 2008, Tucson, AZ, USA, Association for Computing Machinery.

"Securing Software: An Evaluation of Static Source Code Analyzers[9]." Zitser, Misha, Master's Thesis, Massachusetts Institute of Technology, Dept. of Electrical Engineering and Computer Science, 2003.

"Software Assurance Metrics And Tool Evaluation[10]." Black, Paul E., *International Conference on Software Engineering Research and Practice* (SERP), June 2005.

"Source Code Analysis: A Road Map." Binkley, D., *Future of Software Engineering* (FOSE '07), 2007, pp. 115-30, May 23-25, 2007, Minneapolis, MN, USA, IEEE Computer Society.

Source Code Security Analysis Tool Functional Specification[11] Version 1.0, NIST Special Publication 500-268, May 2007

Source Code Security Analysis Tool Test Plan[12] Version 1.0, NIST Special Publication 500-270, January 9, 2008 (DRAFT)

[7] http://samate.nist.gov/index.php/Main_Page.html

[8] http://hissa.nist.gov/%7Eblack/Papers/staticAnalyExper%20Ada%20Geneva%20Jun%20007.html

[9] https://dspace.mit.edu/handle/1721.1/18025

[10] http://hissa.nist.gov/%7Eblack/Papers/samateSERPjun05.html

[11] http://samate.nist.gov/docs/source_code_security_analysis_spec_SP500-268.pdf

[12] http://samate.nist.gov/docs/source_code_security_analysis_test_plan_01_09_08.pdf

“Testing Static Analysis Tools Using Exploitable Buffer Overflows from Open Source Code.” Zitser, M., Lippmann, R., and Leek, T. *SIGSOFT Software Engineering Notes*, Vol. 29, No. 6 (2004), pp. 97-106.

The 2005 Workshop on the Evaluation of Software Defect Detection Tools[13] contains a number of papers that may be of interest for evaluating security analyzers, though the workshop itself is broader in scope.

"The Compiler as a Static Analysis Tool." Dewar, R.B.K. *Ada Letters*, Vol. 37, No. 3, Dec. 2007, pp. 83-87, ACM.

"The Evolution and Decay of Statically Detected Source Code Vulnerabilities." Di Penta, Massimiliano, Cerulo, Luigi, and Aversano, Lerina, *Proceedings - 8th IEEE International Working Conference on Source Code Analysis and Manipulation (SCAM 2008)*, pp. 101-110, Sept. 28-29, 2008, Beijing, China, IEEE Computer Society.

"The Use and Limitations of Static-Analysis Tools to Improve Software Quality." Anderson, Paul, *CrossTalk*, Vol. 21, No. 6, (June 2008), pp. 18-21.

"Using a Diagnostic Corpus of C Programs to Evaluate Buffer Overflow Detection by Static Analysis Tools[14]." Kratkiewicz Kendra, and Lippmann, Richard, *Workshop on the Evaluation of Software Defect Detection Tools*[15], 2005.

Cigital, Inc. Copyright

The Build Security In (BSI) portal is sponsored by the U.S. Department of Homeland Security (DHS), National Cyber Security Division. The Software Engineering Institute (SEI) develops and operates BSI. DHS funding supports the publishing of all site content.

[13] http://www.cs.umd.edu/%7Epugh/BugWorkshop05

[14] http://www.cs.umd.edu/%7Epugh/BugWorkshop05/papers/62-kratkiewicz.pdf

[15] http://www.cs.umd.edu/%7Epugh/BugWorkshop05

[1] mailto:copyright@cigital.com